WHAT IS CLAIMED IS:

1. A public key generation apparatus including:

a random number generator for generating a random number ka that holds a relationship $0 < ka < q$, where an element in a finite group F for which multiplication is defined is g and an order that is a prime number of the element g is q; and

a public key generator for calculating a public key ya in the finite group F from the random number ka, the element g, and the prime number q,

at least said random number generator and said public key generator being formed on one semiconductor integrated circuit, and

a controller of a first user as a distribution source of the public key controlling the random number generator and the public key generator for obtaining the public key ya, and transmitting the obtained public key ya to a second user as a distribution destination of the public key.

2. The public key generation apparatus of Claim 1 wherein

said public key generator calculates the public key ya in the finite group F by a formula: $ya = g^{ka} \bmod q$, using the random number ka, the element g, and the prime number q.

3. The public key generation apparatus of Claim 1 wherein

when the finite group F is an elliptic curve E(F) in a finite

field, and an element of the elliptic curve E(F) is G,

said public key generator calculates the public key ya on the elliptic curve E(F) by a formula: ya = kaG mod q, using the random number ka, the element G, and the prime number q.

4. The public key generation apparatus of any of Claims 1 to 3 wherein

said random number generator generates a new random number ka after the calculation of the public key ya is completed.

5. A shared key generation apparatus including:

a random number generator for generating a random number ka that holds a relationship $0 < ka < q$, where an element in a finite group F for which multiplication is defined is g and an order that is a prime number of the element g is q; and

a shared key generator for calculating a shared key Ka in the finite group F from a public key yb that is generated from a random number kb which holds a relationship $0 < kb < q$ and is generated by a second user as a distribution destination of the shared key, and the random number ka,

at least said random number generator and said shared key generator being formed on one semiconductor integrated circuit, and

a controller of a first user as a distribution source of the shared key obtaining the public key yb from the second user

as the shared key distribution destination, and controlling the random number generator and the shared key generator for deriving the shared key Ka.

6. The shared key generation apparatus of Claim 5 wherein

said shared key generator calculate the shared key Ka in the finite group F by a formula: Ka = yb^ka mod q, using the public key yb = g^kb mod q which is generated by the second user as the shared key distribution destination and the random number ka.

7. The shared key generation apparatus of Claim 5 wherein

when the finite group F is an elliptic curve E(F) in a finite field and an element of the elliptic curve E(F) is G,

said shared key generator calculates the shared key Ka on the elliptic curve E(F) by a formula: Ka = kayb mod q, using the public key yb = kbG mod q which is generated on the elliptic curve E(F) from the random number kb by the second user as the shared key distribution destination, and the random number k.

8. The shared key generation apparatus of any of Claims 5 to 7 wherein

said random number generator generates a new random number ka after the calculation of the shared key Ka is completed.

9. A key exchange apparatus including:

a random number generator for generating a random number ka that holds a relationship 0 < ka < q, where an element in a finite group F for which multiplication is defined is g and an order that is a prime number of the element g is q;

a public key generator for calculating a public key ya in the finite group F from the random number ka, the element g, and the prime number q; and

a shared key generator for calculating a shared key Ka in the finite group F on the basis of the public key yb generated from a random number kb which holds a relationship 0 < kb < q and is generated by a second user as a distribution destination of the shared key, and the random number ka,

at least said random number generator, said public key generator, and said shared key generator being formed on one semiconductor integrated circuit, and

a controller of a first user as a distribution source of the shared key controlling the random number generator and the public key generator for obtaining the public key yb, and controlling the shared key generation unit for deriving the shared key ka.

10. The key exchange apparatus of Claim 9 wherein

said public key generator calculates the public key ya in the finite group F by a formula: ya = g^ka mod q, using the random number ka, the element g, and the prime number q, and

said shared key generator calculates the shared key Ka in the finite group F by a formula: Ka = yb^ka mod q, using the public key yb = g^kb mod q which is generated in the finite group F by the second user as the shared key distribution destination using the random number kb, and the random number ka.

11. The key exchange apparatus of Claim 9 wherein

when the finite group F is an elliptic curve E(F) in a finite field, and an element of the elliptic curve E(F) is G,

said public key generator calculates the public key ya on the elliptic curve E(F) by a formula: ya = kaG mod q, using the random number ka, the element G, and the prime number q, and

said shared key generator calculates the shared key Ka on the elliptic curve E(F) by a formula: Ka = kayb mod q, using the public key yb = kbG mod q generated from the random number kb on the elliptic curve E(F) by the second user as the shared key distribution destination, and the random number ka.

12. The key exchange apparatus of any of Claims 9 to 11 wherein

the random number generator generates a new random number ka after the calculation of the public key ya and the calculation of the shared key Ka are both completed.

13. A key exchange apparatus including:

a random number generator for generating a random number

ka that holds a relationship $0 < ka < q$, where an element in a finite group F for which multiplication is defined is g and an order that is a prime number of the element g is q;

a secret key holding unit for temporarily holding the random number ka;

a public key generator for calculating a public key ya in the finite group F from the random number ka, the element g, and the prime number q; and

a shared key generator for calculating a shared key Ka in the finite group F using a public key yb generated from a random number kb which holds a relationship $0 < kb < q$ and is generated by a second user as a destination distribution of the shared key, and the random number ka that is held by the secret key holding unit,

at least said random number generator, said secret key holding unit, said public key generator, and the shared key generator being formed on one semiconductor integrated circuit,

a controller of a first user as a distribution source of the shared key controlling the random number generator and the public key generator for obtaining the public key ya, and transmitting the obtained public key ya to a second user as a distribution destination of the shared key, and

said controller obtaining the public key yb from the second user as the shared key distribution destination, and controlling the shared key generator for deriving the shared key Ka.

14. The key exchange apparatus of Claim 13 wherein

the public key generator calculates the public key ya in the finite group F using the random number ka, the element g, and the prime number q by a formula: ya = g^ka mod q, and

the shared key generator calculates the shared key Ka in the finite group F by a formula: Ka = yb^ka mod q, using the public key yb = g^kb mod q that is generated in the finite group F from the random number kb by the second user as the shared key distribution destination, and the random number ka that is held in the secret key holding unit.

15. The key exchange apparatus of Claim 13 wherein

when the finite group F is an elliptic curve E(F) in a finite field, and an element on the elliptic curve E(F) is G,

the public key generator calculates the public key ya on the elliptic curve E(F) using the random number ka, the element G, and the prime number q by a formula: ya = kaG mod q, and

the shared key generator calculates the shared key Ka on the elliptic curve E(F) by a formula: Ka = Kayb mod q, using the public key yb = kbG mod q that is generated from the random number kb on the elliptic curve E(F) by the second user as the shared key distribution destination, and the random number ka that is held in the secret key holding unit.

16. The key exchange apparatus of any of Claims 13 to 15 wherein the random number generator generates a new random number ka after the calculation of the public key ya is completed, and the secret key holding unit holds the new random number ka generated by the random number generator.

17. The key exchange apparatus of any of Claims 13 to 15 wherein the random number generator generates a new random number ka after the calculation of the shared key Ka is completed, and the secret key holding unit holds the new random number ka generated by the random number generator.

18. A key exchanging method that employs the key exchange apparatus of any of Claims 9 to 17, thereby exchanging the public keys that are generated by a first user and a second user that intend to exchange the public keys, respectively, to generate a shared key by the first user and the second user on the basis of the exchanged public key, respectively.